THOMAS COOPER

"The quality and breadth of Thomas Cooper's expertise is truly vast…Professional, excellent communicators who are "in tune with the industry."
Chambers & Partners Legal Directory

Non-Affirmative/Silent Cyber Issues: an overview (marine business)

Rhys Clift, Partner

London
Madrid
Paris
Piraeus
Singapore

www.thomascooperlaw.com


VIRUS
DETECTED


malware worm trojan virus spam hackers spyware security rootkit phishing

Outline: an overview of silent cyber issues (marine)

- What is cyber risk?
- What are the (UK) regulatory drivers to assess risk?
- What is affirmative and non-affirmative risk/cover?
- What are the types of cyber incident?
- What are the types of cyber losses?
- What is the market approach to exclusions?

- What is CL380?
- What are the criticisms of CL380?
- What is the IMIA Advanced Cyber Exclusion clause?
- How might the impact of the CL380 approach be moderated?
- What new exclusions are being drafted?
- Conclusions

What is cyber risk?

- No standard definition
- OECD Report ***"Enhancing the role of insurance in Cyber Risk Management, 2017"*** quotes two definitions:
- ***"any risks that emanate from the use of electronic data and its transmission, including technology tools such as the Internet and telecommunications networks"*** **–** Chief Risk Officers Forum (2014).

- ***"any risk emerging from the use of information and communication technology that compromises the confidentiality, availability, or integrity of data or services" –*** Geneva Association (2016) –insurance industry think tank (45 yrs).

- Per OECD both include risks related to human error and intentional/malicious acts, internal or external ***(nations states, terrorists, industrial competitors, organised crime, hacktivists or lone hackers/criminals)***.

- IT hardware/software systems are **endemic/all pervasive**
  - the Internet,
  - governmental,
  - industrial,
  - commercial,
  - domestic...
- The foundation of astonishing, fundamental change and improvement, but presenting huge risk, known and unknown
- Huge business opportunity in insurance?

- But, serious concern about insurance and reinsurance contracts exposed to cyber related losses of two main types:
  - Malicious acts: say cyber attack, infection of IT system with malicious code
  - Non-malicious acts: say loss of data, accidental acts or omissions
- Merits new approach to terms of:
  - Coverage?
  - and
  - Analysis of claims?

THOMAS COOPER

What are the (UK) regulatory drivers to assess risk?

- Substantial work conducted/required by Bank of England Prudential Regulation Authority:
- Cross-Industry review: conducted 10/15 to 6/16
- Key findings: Cyber Underwriting Risk, BOE PRA, November 2016
- Supervisory Statement: BOE PRA, July 2017
  - Safety and soundness of insurers
  - Appropriate degree of protection for policyholders

- Follow up survey: BOE PRA, May 2018
- Follow up survey results, Cyber Underwriting Risk, BOE PRA January 2019:
- More needs to be done..
- To reduce unintended exposure to non-affirmative cyber risk insurers need to develop action plan by H1 2019 with milestones and dates for action
- Notes underwriters concerns : market conditions, broker pressure, lack of historical data, models and expertise

What is affirmative and non-affirmative cyber risks/cover?

- Affirmative:
  - Those that explicitly include cover for cyber risk
  - (Tight terms, low limits)
- Non-Affirmative (silent):
  - **“Those that do not explicitly include or exclude”**

- BOE PRA expects firms to **identify, quantify and manage** cyber insurance underwriting risk (SS July 2017) in both categories.
- But Non-Affirmative may present greatest risks
  - Unknown unknowns?
  - Risk of nasty surprises
  - Policy disputes

- Hence BOE PRA main expectations July 2017 has three broad areas of focus:
  - **Non-affirmative cyber risk**
  - Cyber risk strategy and appetite
  - Cyber expertise (continuous updating of knowledge and understanding)

- Non-affirmative cyber risk, the principal area of concern. Hazard of unintended exposure to risk to be managed e.g. by:
  - Adjustment to premium
  - Adjustment/fixing of limits
  - **Use of robust wording exclusions**

THOMAS COOPER

How might cyber risk affect ship systems?

Ship Visitors	USB Drives	Laptops	Phones
Pilots	Port and Terminal Employees	Engineers and Technicians	Suppliers

- Bridge systems – Electronic Chart Display and Information System (ECDIS), Automatic Information System (AIS) and Global Positioning System (GPS)
- E Navigation ? Update on line?
- Remote machinery diagnostics /maintenance?

What are the types of cyber incidents?

- OECD (Report, 2017) listing of common types of cyber incident:
  - Data confidentiality breach (own or third party)
  - **Operational technology malfunction**
  - Network communication malfunction
  - Inadvertent disruption of third party system

- Disruption at external service provider
- Deletion or corruption of data
- Encryption of data
- Cyber fraud/cyber threat

THOMAS COOPER

What are the types of cyber losses?

- OECD names as potential losses in the OTM category ***"physical asset damage"***
- But OECD examples are all non-marine:
  - 2008 pipeline explosion (safety systems disabled), Turkey
  - 2010 centrifuge damage (control systems disabled), Iran
  - 2014 damage to blast furnace (ditto), Germany
  - 2015 damage to electricity network (ditto), Ukraine

- From the OECD listing:
  - ***Operational technology malfunction***
- For physical loss and damage
- Perhaps most likely to be of interest in the ownership and operation of marine vessels and yachts?

- For example OTM maybe:
  - Damage to navigation, propulsions systems, control systems of machinery?
  - Causing fire, explosion, grounding, collision?
- But (new) difficulties with ascertainment/proof of proximate cause?
- Do computer failures etc cause fire, explosion etc?
- What is the proximate cause? Competing causes crew negligence, defect in design? Others?

THOMAS COOPER

What are the (other) types of cyber losses?

- This is not to ignore (but not the main focus today):
- Potential claims for **loss of use** on say LOU cover? Where yacht chartered out?
- Potential claims for **ransom** (cyber fraud) on say K&R cover? (Very) different terms and conditions?
- Potential claims for **economic loss** on say managers E&O though cyber theft? (ditto)

What is the market approach to exclusions?

- On a snap shot assessment seems to be:
  - No coherent approach to drafting of exclusions
  - Apparent lack of uniformity/information sharing
  - No agreement /approach within classes
  - No agreement /approach across classes

- Perhaps different classes of business need differing provision?
- Clear marine and non-marine quite separate/different.
- In marine key market exclusion is CL380, published in 2003
- Lately further drafting of exclusions underway
  - Cargo
  - Hull

What is CL380?

- *"1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss damage liability or expense **directly or indirectly caused** by or contributed to by or arising from the use or operation, **as a means of inflicting harm**, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.*

- *1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system, or computer software programme, or any other electronic system* ***in the launch and/or guidance system and or firing mechanism of any weapon or missile".***

What are the criticisms of CL380?

- The following criticisms have been expressed, for example that it is:
  - **Not wide enough**: excludes deliberate but not accidental cyber risk (accidental may be major exposure?)
  - **Too tough on underwriters**: Puts heavy burden on underwriters to prove *"as a means of inflicting harm"*
  - **Unworkable**: Is otherwise an exclusion very widely expressed and may be difficult to persuade court to give effect

- Note that some brokers oppose the use of CL380.
  - A means of protecting insureds
  - And themselves?
- But there are tougher clauses out there (resisted by the brokers and (not yet?) imposed by underwriters?)
- A non-marine example…

What is IMIA Advanced Cyber Exclusion Clause 2017?

1. Any loss, …directly or indirectly caused by or contributed to or resulting from the cyber incidents …in the following provisions a) to g) are not covered …:

- a) **Damage to or Loss of Data occurring on the Insured's Computer Systems**
- b) Computer Malicious Act on the Insured's Computer Systems, or
- c) Computer Malware on the Insured's Computer Systems, or

- d) **Human Error affecting the Insured's Computer Systems**
- e) **System Failure occurring on the Insured's Computer Systems**
- f) **Defect of the Insured's Computer Systems**
- g) Cyber Extortion

How might impact of CL380 approach be moderated?

- By write back for Targeted Cyber Attack?
- Specie Clause JS2018-001 text as per CL380 above then:
- *"1.3 It is understood and agreed that Clause1.1 shall not apply to an otherwise covered physical loss of or physical damage to the assureds property caused by a* ***Targeted Cyber Attack.*** *The burden of proving cover under this write-back shall be on the Insured.*
- *For the purpose of Clause 1.3 Targeted Cyber Attack means the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system where the motive is to inflict harm solely on (or upon) the Insured or the Insured's property".*

- By the use of different terms?
  - Warranties as to:
    - IT systems, (hardware/software)
    - Business methods
    - Personnel training
    - Others?
  - Conditions precedent?
  - Others?

- Possible wholly different method:
- All embracing exclusion of cyber risk from standard marine policies
- Pushing assureds to purchase affirmative cover?
- Disadvantages:
  - Costly for assureds?
  - Inadequate cover (limits/terms) for assureds?
  - Loss of market for underwriters?

What new exclusions are being drafted?

- In Cargo and Hull
- Hull:
  - Might contemplate text of CL380 as above then effectively making write back of cover on a perils basis:
  - Perils of seas, fire, explosion, collision liability etc
  - Plus cover for Targeted Cyber Attack (as defined)?

- But lack of speed or progress probably attributable to:
  - lack of claims
  - lack of serious perceived risk
- Principal driver for change is disaster not innovation.
- Lack of disaster to drive change (in marine)

Conclusions

- Cyber risk: a huge field, a huge (insurance) business opportunity, a huge hazard
- A cause of concern to BOE PRA; pressure to identify, quantify and manage
- Non-Affirmative cyber risk/cover (silent cyber) a particular cause for concern. Unknown unknowns?
- Might cause physical loss and damage to ships/yachts. But query insurance policy impact. Proximate cause? A reason for a new approach to investigation and proximate cause?
- Might be the cause of economic losses; loss of use, ransom, E&O exposure? Query terms of cover

- No uniform market approach to exclusions
- Main exclusion CL 380: old, the subject of criticism, due for reform/amendment?
- (Much) tougher exclusions exist (in draft), but unusable because of market conditions?
- CL380 might be moderated by write back or the use of other contract terms (warranties or conditions precedent)?
- New exclusions under consideration. But lack of strong driver for change?

Sources highlight Thomas Cooper's quality lawyers and international reach…
Chambers & Partners

For further information or advice, please contact:

Rhys Clift
Email: rhys.clift@thomascooperlaw.com
Direct: +44 20 7390 2222
Mobile: +44 77 1348 8019

www.seamediation.com